DE ELEKTRONISCHE IDENTITEITSKAART

Vloek of zegen?

De voorbije maanden werden bijna twee miljoen belastingaangiftes ingediend via tax-on-web. De elektronische identiteitskaart werd veelal gebruikt om in te loggen. Tegen het eind van het jaar moeten alle Belgen zo'n eID hebben. De mogelijkheden zijn legio. De gevaren ook.

Door Vincent NAESSENS en Bart DE DECKER

Eind 2009 zal elke Belg ouder dan 12 jaar een identiteitskaart met chip op zak hebben. Daarmee kunnen ze zich elektronisch identificeren, authenticeren en digitale handtekeningen plaatsen op elektronische documenten. Maar alle andere kaarten in je portefeuille zal de eID niet vervangen. En de kaart onverstandig gebruiken houdt ook gevaren in.

Verzekeringen en inbrekers

De kaart bevat verschillende bestanden met identificatie- en adresgegevens die uitgelezen kunnen worden zodra je de kaart in een lezer stopt. Dat uitlezen wordt niet afgeschermd. Dat betekent dat je geen pincode hoeft in te geven. Op de website van de overheid vind je software die de uitlezing mogelijk maken. Deze kaartfunctie wordt vaak gebruikt om gegevens van personen (zoals naam, adres, foto, ...) sneller te verwerken aan registratiedesks. Denk maar aan de registratie in hotels of bij de notaris. Ook in sommige containerparken moet je je eID laten uitlezen om toegang te krijgen, en soms weet men zo ook op welke rekening de kosten geboekt mogen worden.

Hoewel je met de elektronische identiteitskaart lange wachtrijen kan vermijden, moet je er toch voorzichtig mee omspringen. Zodra je je kaart in de lezer stopt, kan immers heel wat persoonlijke informatie gelezen worden, zoals je rijksregisternummer. Met dit unieke identificatienummer kunnen heel wat gegevens aan elkaar gelinkt worden. Een winkelketen kan het nummer bijvoorbeeld gebruiken om voor elke klant een profiel van zijn consumptiegedrag op te bouwen. Een verzekeringsagent kan alle polissen van een cliënt linken aan het identificatienummer. Bovendien worden steeds meer gegevens uitgewisseld tussen dienstverleners. Als de verzekeringsagent en de winkelketen hun profielen zouden uitwisselen, dan kunnen mensen met een ongezonde levensstijl hun verzekeringspremie wel eens de hoogte in zien gaan.

Bij registratie is misschien alleen je naam belangrijk. Toch zijn ook andere gegevens, zoals je foto of adres, te zien. Het is dus heel belangrijk dat je vertrouwen hebt in de persoon of instelling die je identificatiegegevens wil uitlezen. Stel jezelf de vraag 'Vind ik het erg dat deze persoon of instelling mijn identificatiegegevens (inclusief adres en foto) kan uitlezen?' Als het antwoord ja is, dan is het gebruik van de kaart af te raden.

Bovendien moet je ook vertrouwen hebben in de computer waarmee de kaartlezer verbonden is. Een pc zonder up-to-date antivirus- en antispywareprogramma raakt heel snel besmet als hij verbonden is met het Internet. Schadelijke programma's kunnen onbeperkt je persoonlijke gegevens uitlezen en doorsturen naar om het even welke computer. Zo overwegen steeds meer fitness- en saunacentra de eID te gebruiken aan de ingang. Als op hun computer spyware draait, die per ongeluk of moedwillig is geïnstalleerd, dan kunnen de klantgegevens, waaronder het adres, doorgestuurd worden naar criminele organisaties. Die weten dat de klant een paar uur niet thuis zal zijn: een mooie gelegenheid om zijn huis een 'bezoekje' te brengen.

Identificatie met de eID-kaart is zeker niet geschikt als de veiligheid erg belangrijk is. Het identificatiebestand kan immers op elk werkstation - pc of laptop - uitgelezen worden. De uitgelezen gegevens kunnen dan gekopieerd worden naar een andere smartcard. Zo zou een inwoner uit Halle zich met een gekopieerde kaart van een inwoner uit Vilvoorde kunnen aanmelden in het containerpark van Vilvoorde en zo veel meer afval kwijt kunnen. Akkoord, dit is misschien niet zo problematisch. Maar de identificatie met de eID gebruiken om toegang te verschaffen tot kritische delen van een kerncentrale is allerminst aangewezen.

Belastingen

Elektronische authenticatie wordt vaak toegepast bij het inloggen op websites (zoals tax-on-web) en vervangt omslachtige procedures met paswoorden. Bij authenticatie bewijst een gebruiker dat hij

eigenaar is van de identiteitskaart. Dat gebeurt in een aantal stappen. Eerst zendt de server een authenticatieverzoek naar je werkstation. Dat verzoek wordt doorgestuurd naar je eID-kaart. Vervolgens worden op de kaart een aantal cryptografische bewerkingen uitgevoerd met een private sleutel. Deze sleutel kan niet uitgelezen (en dus ook niet gekopieerd) worden. Voor je kaart de bewerkingen kan uitvoeren, moet je eerst je pincode ingeven. Ten slotte gaat het resultaat van de cryptografische bewerkingen terug naar de (web)server, samen met het autenticatiecertificaat. De webserver kan zo de authenticiteit van de gebruiker nagaan. Het authenticatiecertificaat bevindt zich op de chip en bevat een aantal persoonlijke gegevens (zie kaderstuk).
Elektronische authenticatie geeft gebruikers toegang tot heel wat persoonlijke informatie zoals financiële gegevens (belastingaangiftes en loonfiches), gegevens die over jou worden opgeslagen in het rijkregister (zoals je rijbewijs en gezinstoestand), ... En dat zullen er alleen maar meer worden. Om het allemaal niet te omslachtig te maken, hoef je maar één keer je pincode in te geven. Nadien kan je zonder code inloggen op andere websites, zolang je kaart maar in de lezer blijft zitten.
De pincode maakt authenticatie veiliger dan identificatie. Toch is ook hier waakzaamheid geboden. Een kwaadaardig programma op je pc kan detecteren of je je pincode al hebt ingegeven. Als dat zo is, kan dat programma zonder dat je het weet inloggen op webservers zoals tax-on-web of myminfin (hier zijn financiële gegevens zoals je loonfiches beschikbaar), je persoonlijke gegevens afhalen en vervolgens verder doorsturen.
Ook nu is het dus erg belangrijk dat je het werkstation waarmee je inlogt volledig kunt vertrouwen. Dat is zeker niet altijd het geval op publieke computers. Bovendien volstaat het niet om je eigen pc te beveiligen. Je moet ook de dienstverlener kunnen vertrouwen die om authenticatie vraagt. Inloggen op dubieuze websites die irreële kortingen aanbieden is geen goed idee. Het kan niet alleen leiden tot het ophalen van je identificatiegegevens op de kaart zelf, maar ook tot het verlies van persoonlijke informatie uit overheidsdatabanken.

Digitale handtekening.

Je kan de elektronische identiteitskaart ook gebruiken om een digitale handtekening te plaatsen. Dat kan heel wat tijdwinst opleveren bij administratieve diensten: documenten hoeven niet meer afgedrukt te worden en per post of fax doorgestuurd. Het principe is gelijkaardig aan authenticatie. Je stuurt een aanvraag naar de kaart om een digitaal document te ondertekenen. Je geeft de pincode in en het document is getekend.
Ook hier zitten echter een aantal aan addertjes onder het gras. Om waardevolle documenten zoals contracten te ondertekenen moet een betrouwbare timestamp (of 'datering') toegevoegd worden aan het document. Zo'n timestamp duidt het tijdstip aan waarop het document ondertekend werd. Voor een betrouwbare datering is een derde partij vereist. Anders zou een gebruiker een timestamp kunnen toevoegen van een toekomstig tijdstip, en onmiddellijk na het plaatsen van de handtekening zijn eID laten intrekken – door aan de overheid te melden dat hij zijn kaart heeft verloren. Zo kan hij de geldigheid van het contract betwisten.
Ook nu moet je erg voorzichtig zijn op andere werkstations, waarbij je gevraagd wordt de pincode via het toetsenbord in te geven. De code kan immers met misleidende software worden opgeslagen. Dat verschilt grondig met huidige bankkaarten (waarbij de pincode ofwel op een betrouwbare terminal of op een speciaal pinpadapparaat wordt ingegeven). Bovendien heb je op onbetrouwbare werkstations geen absolute zekerheid over welk document je ondertekent. Een makelaar kan een contract voorschotelen maar stiekem een aangepast contract ter ondertekening naar de kaart sturen.

The Sky is the Limit?

De eID-kaart biedt heel wat interessante mogelijkheden. Nieuwe toepassingen maken persoonlijke informatie toegankelijker of vereenvoudigen administratieve taken. Met de introductie van de kaart is België bij de koplopers op het gebied van eID-technologie in Europa. Toch zijn de mogelijkheden niet oneindig. Het zal nog een tijd duren voor alle andere kaarten overbodig worden.
Zowel ontwikkelaars van toepassingen als de gebruikers moeten omzichtig omspringen met de eID-kaart. Net zoals bij een bankkaart kan je persoonlijke schade oplopen als je je identiteitskaart onverstandig gebruikt. Belangrijkste is je werkstation goed beveiligen en een goede inschatting maken van de omstandigheden waarin je persoonlijke informatie wil prijsgeven aan dienstverleners.

(kadertje)

Wat staat er op mijn eID?

Identificatiebestand
- Naam en voornaam
- Rijksregisternummer
- Nationaliteit

- Geboortedatum en -plaats
- Geslacht
- Kaartnummer
- Chipnummer
- Adresgegevens
- Foto
- ...

Authenticatiecertificaat
- Naam en voornaam
- Rijksregisternummer
- Nationaliteit
- Serienummer
- Publieke sleutel
- ...

(kadertje)

Checklist voor veilig gebruik

- Is het werkstation up-to-date beveiligd?
- Kan ik het werkstation voldoende vertrouwen?
- Mogen persoonlijke gegevens op het werkstation worden opgeslagen?
- Is de dienstverlener te vertrouwen?
- Heeft de dienstverlener mijn gegevens echt nodig voor de aangeboden dienst?
- Kan de dienstverlener mijn gegevens misbruiken?